

Mr/Mrs [●]
Examining Judge
Court of First Instance of [●]
Belgium

Brussels, [●] 2013

Dear Examining Judge,

Subject : **CRIMINAL COMPLAINT AGAINST DOMIEN NOWICKI FOR
ALLEGED HACKING OFFENCES**
Registration of a civil claim by Nintendo, as an injured party
O. ref. : R.0026

NINTENDO CO, LTD., with its registered offices at Kyoto-shi-Kyoto-fu, 607
Fukuiine Kamitakamatsu-cho, Higashiyama-Ku, Japan

hereinafter “Nintendo”;

electing domicile at the offices of their counsel, Mr Olivier Vrins, attorney-at-law at
ALTIUS, avenue du Port 86C, B.414, 1000 Brussels, Belgium, for the purpose of the
present complaint, in accordance with Article 68 of the Criminal Investigation Code;

hereby file a criminal complaint, registering Nintendo as an injured party with a civil
claim against **DOMIEN NOWICKI** (hereinafter “the defendant”), based on the following
allegations:

1. FACTS

A. THE NINTENDO 3DS CONSOLE

1. On 25 March 2011, Nintendo Co., Ltd. (hereinafter: “Nintendo”) launched the latest version of the Nintendo DS family of handheld video game consoles in Europe, the Nintendo 3DS (hereinafter the “3DS”). The new console offers consumers new functionalities as well as the ability to view and play games in 3D.



(Nintendo 3DS console, source: www.nintendo.com)

The 3DS is also backwards compatible, which means that a distinct operating system (“DS mode”) enables consumers to play games developed for the earlier Nintendo DS and DSi consoles on the 3DS. This “DS mode” is separate from the “3DS mode” which enables the playing of 3DS games.

The Nintendo 3DS is a multi-functional, handheld computer gaming device that, in addition to game play, facilitates other operations commonly associated with smartphones, tablets and other computers. The 3DS CPU is a 1Ghz dual-core ARM11 Mpcore chip from the same processor family that supports products such as the Apple iPhone, iPod Touch, Amazon Kindle 2, Nokia tablet devices and numerous other smartphones. It features 2GB of internal memory and uses the SD memory card format to allow further storage of data on SD flash memory cards.

The 3DS features dual screens, one of which acts as a touchscreen operable by finger or stylus. It also contains a wireless communication system (WiFi), providing users the ability to automatically locate and connect to WiFi-hotspots for data sharing; via WiFi connection, the 3DS enables users to browse the web, join multiplayer online

gameplay, purchase and download game software and other computing applications through Nintendo's "eShop." Additionally, the device's built-in cameras provide users the opportunity to take 3D pictures and capture video. Similarly, the 3DS is also capable of audio (e.g. MP3s) and video playback (e.g. content from the 3DS and streamed from applications such as Netflix and Hulu Plus¹).

2. Hacking, modifying or accessing the hardware or software of the 3DS game console or 3DS games is not authorized by Nintendo.

This clearly follows from, *inter alia*, the information on the 3DS Service User Agreement and Privacy Policy ("EULA"), the 3DS's Hardware Packaging, Hardware Operation Manual and Software Packaging. The EULA states:

*"Your use of the Nintendo 3DS Services is subject to your full compliance with this Nintendo 3DS Code of Conduct (...). **The Nintendo 3DS Code of Conduct prohibits all harmful, illegal or otherwise offensive conduct, including, but not limited to the following: (...) Hosting, intercepting, emulating, reverse engineering any part of the Nintendo 3DS System or the Nintendo 3DS Services or redirecting the communication protocols used by Nintendo as part of the Nintendo 3DS Services, regardless of the method used to do so.**"*

Moreover, the access to the inside of the console is blocked by a closed outer shell.

This is finally confirmed by the presence of technological protection measures implemented on the 3DS and authentic 3DS games (see further below in this regard).

3. Nintendo has made considerable investments in order to conceive, develop and market the 3DS. It has also made such investments, as have done independent game developers, with regards to the 3DS games.

As follows from the above, security is a crucial issue for Nintendo when developing its consoles. The measures developed by Nintendo are, among other, aimed to prevent the playing of unauthorized copies of Nintendo games (and thus to fight piracy), to prevent users from breaching warranties on the 3DS console, and to prevent consumers from opening up the console and the hazards inherent in doing so with a highly technical electronic device.

B. THE 3DS HACKING ACTIVITIES PERFORMED BY DOMIEN NOWICKI

4. The 3DS mode's security has until now remained intact thanks to the important barriers established by Nintendo.

However, some time ago, Nintendo discovered that an individual nicknamed "Neimod" had been actively seeking to hack the 3DS (and in particular the 3DS mode) and

¹ Both applications are currently available to US consumers only

reporting on his activities and achievements using Internet Relay Chat ("IRC") on a particular IRC channel called EFNET's #3dsdev channel. This is a publicly available and accessible channel that is well-known in the hacking community and where hackers and others associated with the hacking community visit and communicate with one another concerning the latest attempts to hack, in this case, the 3DS console. Although a specialist channel, anyone around the world may access and read the comments that are posted there.

In the IRC conversations, "Neimod" wrote, among others, the following (emphasis added; larger excerpts are provided as exhibits to this complaint):

- [2012/02/23 12:32:31] <neimod> **today is a good day for haxx** though
- 13[2012/03/12 18:05:47] <neimod> i'm refactoring the old dsi ram tracer code
13[2012/03/12 18:06:10] <neimod> so i can add support for my uploading my own patching code
- 13[2012/03/18 19:59:39] <balrog> they really leave debug code in? hahahahahaha
[2012/03/18 20:00:05] <neimod> yup
13[2012/03/18 20:00:32] <neimod> they make this nice restricted OS/kernel, but hand you the keys to break free too
[2012/03/18 20:01:00] <neimod> but only if you know where to look :)
- [2012/03/02 13:37:43] <neimod> <http://i.imgur.com/08BGq.jpg>
- [2012/03/22 17:42:21] <neimod> it's still all done with the flick of a switch
[2012/03/22 17:51:18] <joink> neimod: so when are you going into mass production?
[2012/03/22 17:51:24] <joink> how much for "modding" my 3DS :)
(...)
[2012/03/22 18:18:18] <Luigi__> well, all that heap of electronics is nice, but I'd use it if it could fit into a cartridge :P
(...)
[2012/03/22 18:24:37] <neimod> when i have my own factory and a thousand asians working for me
- [2012/10/06 19:10:40] <PRIZZA> **neimod are you hacking a PAL 3ds?**
[2012/10/06 19:11:13] <Yuuki> should i buy lego 3 ? xd
[2012/10/06 19:11:45] <@neimod> **well of course, i have only european 3ds**
[2012/10/06 19:12:41] <PRIZZA> neimod, are you on to something?
[2012/10/06 19:13:09] <@neimod> always
- [2012/12/17 20:11:14] <@neimod> sorry, **no mediocre programmers allowed in the secret circle**
[2012/12/17 20:11:35] <Joostin> **I would be of no use in the actual hacking**
- [2012/12/25 05:13:21] <@neimod> nope, this is for an unmodified 3ds
[2012/12/25 05:13:32] <@neimod> the only thing modified is the gamecard
[2012/12/25 05:13:53] <@neimod> (to allow communication with PC)
[2012/12/25 05:13:59] <bob_> and you can read and write physical addresses?
[2012/12/25 05:14:03] <@neimod> yup
13[2012/12/25 05:14:31] <bob_> you have a kernel exploit?
[2012/12/25 05:15:05] <@neimod> sortof
13[2012/12/25 05:15:55] <@neimod> it's as good as a kernel exploit :)
[2012/12/25 05:16:02] <@neimod> same functionality
- [2012/12/30 05:28:18] <@neimod> what do you guys think. would this work correctly?
<http://pastie.org/private/zkzt1ij6hxn3s4xwnjnwca>
[2012/12/30 05:29:26] <@neimod> trying to create a communication link between the arm11s and arm9 via memory

- [2012/12/22 21:10:24] <@neimod> paypal has unfrozen the funds from the fundraiser
[2012/12/22 21:11:08] <@neimod> and donating by paypal option will soon be added again
 - [2012/04/06 21:24:22] <neimod> hehe, got the 3ds displaying "tetestminstellingen" instead of "Systeeminstellingen" ;)
[2012/04/06 21:25:18] <balrog_> :U
[2012/04/06 21:25:20] <balrog_> :O *
[2012/04/06 21:25:23] <balrog_> awesome, how
[2012/04/06 21:26:12] <neimod> patching ofcourse!
[2012/04/06 21:26:19] <neimod> mario kart here i come!
 - [2012/04/06 20:52:31] <neimod>
<http://www.flickr.com/photos/neimod/4860594669/in/photostream>
5. From time to time, Nintendo updates the firmware on the 3DS console through releasing what are referred to as System Menu Updates ("SMUs"). SMUs often contain enhancement for game play or other functionality (such as updating parental controls). SMUs may also contain security updates. Further background and a history to the different versions of SMUs previously released can be found at http://www.nintendo.com/consumer/systems/dsi/en_na/systemMenuFeatures.jsp
6. Consumers must consent to and download the latest SMU released by Nintendo. The latest SMU for the 3DS console was released on 26 March 2013.
5. On the same day as the SMU release there was interesting chatter on the IRC channel, in which one can see how the hacking community reacts to and seeks to overcome any security updates in the latest SMU release.. The IRC conversation excerpt hereunder (in full as Exhibit), in which the participants discuss the most recent 3DS SMU offers an insight into the "cat and mouse game" played out globally between Nintendo and the hacking community and shows the clear intentions of the "hacking community" in which "Neimod" operates.
- [2013/03/26 17:18:46] <sohakes> So maybe they overlooked some vulnerabilities haha?
[2013/03/26 17:18:55] <trap15> some is probably an understatement
[2013/03/26 17:19:24] <Muzer> oh, nvm
[2013/03/26 17:19:27] <Muzer> didn't think it through fully
[2013/03/26 17:19:27] <sohakes> haha, yeah, probably there are other ways :P
[2013/03/26 17:24:44] <yellow8> yeah there's other potential code exec vulns, didn't get anywhere with those so far though.
[...]
[2013/03/26 19:27:42] <pa1n> anyone know if it's safe to update to 5.0.0-11?
[...]
[2013/03/26 19:32:01] <crowell> pa1n: "Multiple NATIVE_FIRM code execution vulnerabilities were fixed.
[2013/03/26 19:33:13] <Muzer> pa1n: it blocks the exploits that were used. Whether or not there will be more
remains to be seen, but I expect there will be
[2013/03/26 19:33:49] <Muzer> I dunno whether the exploits that were blocked could in the future have been used
for more complete hardware access or anything, though, I haven't really looked into understanding this system.
[2013/03/26 19:35:41] <pa1n> So neimod's exploit got patched as well?
[2013/03/26 19:35:57] <crowell> neimod's hardware exploit didn't get patched
[...]

[2013/03/27 16:10:45] <yellow8> those fixed code exec vulns wouldn't be used in a public release anyway, even if those weren't fixed.

[2013/03/27 16:11:08] <Joostin> so there is no reason not to update?

[2013/03/27 16:11:31] <Joostin> at least for us simple folk

[2013/03/27 16:11:32] <Joostin> lol

[2013/03/27 16:12:57] <yellow8> not sure if anything was fixed/blocked(like the savehax itself) outside of NATIVE_FIRM though.

6. On the online photo gallery of "Neimod", referred to by the latter in the IRC conversation there is, among others, the following pictures named "**HAXXXXXX!!!**"² and "3DS-PC communication link"³ (more screenshots are provided as exhibits to this complaint):

² The caption of the picture (dated 12 October 2012) further states: "*Look closely to the number of studs. This is after clearing only 4,6% of the game. Oh, and by the way... did I mention this is with an unmodified 3DS? ;-)*".


³ The caption of the picture (dated 23 December 2012) further states: "*used an FPGA to 'enhance the savechip as a communication link. This is with an unmodified 3DS, no hardware modification except for the gamecard that exposes the SPI savechip pins.*"

http://www.flickr.com/photos/neimod/8078325837/in/photostream/

La conjugaison du verbe requérir - conjuguer requérir

flickr from YAHOO! The Tour Sign Up Explore Upload Sign In

Favorite Actions Share Newer Older




By neimod
Mister neimod + Add Contact

This photo was taken on October 12, 2012 using a Canon PowerShot G10.

17,091 views 20 comments

This photo belongs to

neimod's photostream (189)



Additional info

Settings: 1/60 f/3.5 ISO 200 15.7 mm

License

© All Rights Reserved

Privacy

This photo is visible to everyone

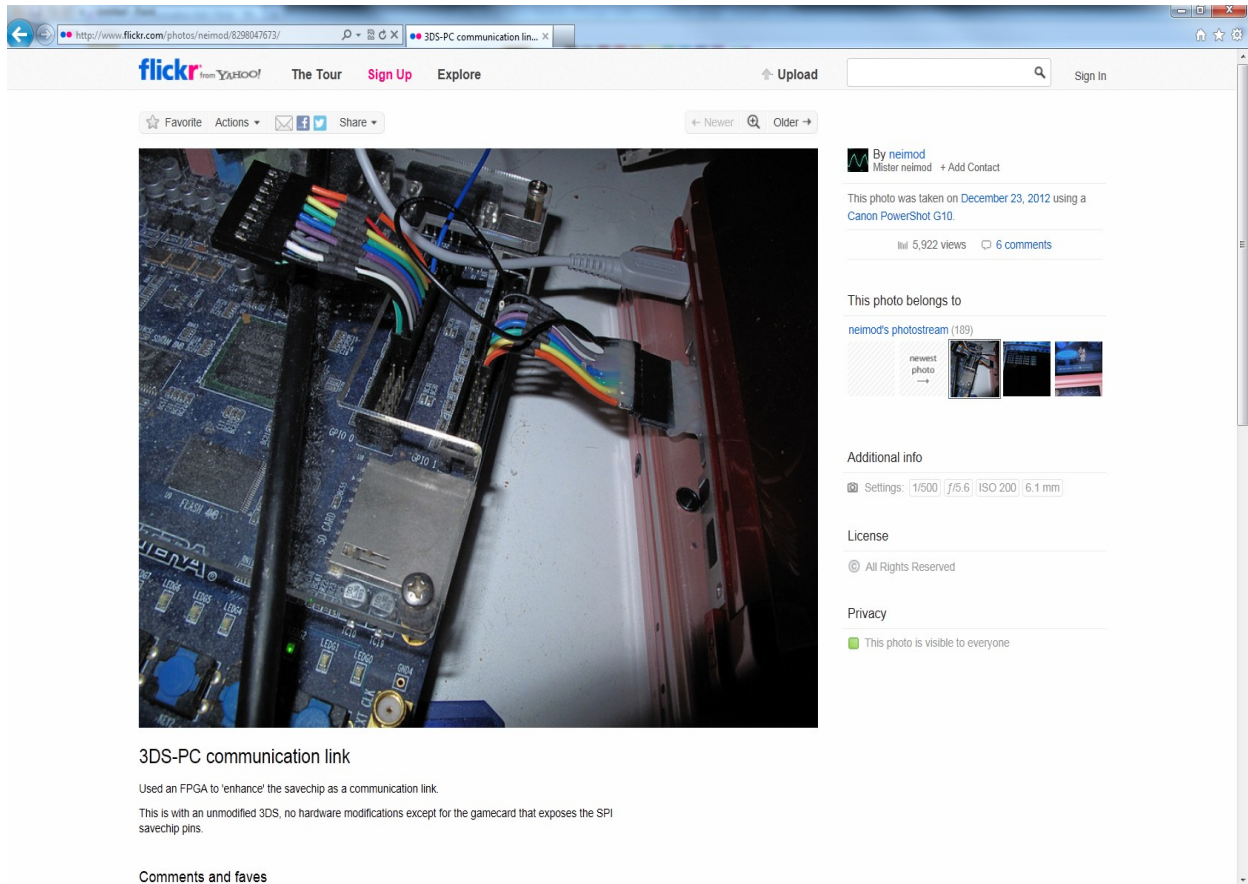
HAXXXXX!!!

Look closely to the number of studs. This is after clearing only 4.6% of the game.

Oh, and by the way... did I mention this is with an unmodified 3DS? :-)

Comments and faves

lance D 2 (2 months ago)



3DS-PC communication link

Used an FPGA to 'enhance' the savechip as a communication link.
This is with an unmodified 3DS, no hardware modifications except for the gamecard that exposes the SPI savechip pins.

Comments and faves

By neimod
Mister neimod + Add Contact

This photo was taken on December 23, 2012 using a Canon PowerShot G10.

5,922 views 6 comments

This photo belongs to
neimod's photostream (189)

Additional info
Settings: 1/500 f/5.6 ISO 200 6.1 mm

License
© All Rights Reserved

Privacy
This photo is visible to everyone

“Neimod” also referred to the following picture in the IRC conversation, on which a 3DS displaying the words “WE HACKED IT!” appears:



7. The IRC conversations and pictures show that Neimod is hacking the Nintendo 3DS, that he is accessing the 3DS' system and circumventing its technological protection measures, and that he is bringing modifications to the hardware and/or software of the 3DS.

8. According to the information that Nintendo has been able to gather, "Neimod" is the appropriate defendant as identified on page 1 of this complaint. Neimod has been identified as Domien Nowicki through a combination of online research, publicly available resources and finally through physical investigations in various locations in Belgium. Preliminary online research identified Neimod as Domien Nowicki who was believed to be, or have been, studying at Hasselt University, Hasselt, Belgium (see Annex []). Investigators engaged by Nintendo (Fusion 85 Limited) searched local telephone directories in an attempt to identify Domien Nowicki and his family. A number of listings were profiled, researched and shortlisted and further enquiries led to the identification of an individual matching the description and photograph of Domien Nowicki obtained previously (see Annex).]

2. OFFENCES

9. "Neimod's acting is constitutive of the following offences under the Belgian Criminal Code. Nintendo reserves its rights to point at further offences in the course of investigation.

A. (ATTEMPT OF) EXTERNAL HACKING (ARTICLE 550**BIS** (1) AND (4) CRIMINAL CODE)

Belgian Criminal Code, Article 550**bis** (1) and (4):

(1) Anyone who, knowing he/she is not authorized, gains access to a computer system or maintains such access, will be punished by between 3 months' and 1 year's imprisonment and/or a fine of between 26 and 25,000 euros.

If the offence outlined in (1) above is committed with fraudulent intent, the term of imprisonment will be between 6 months and 2 years. (...)

(4) Any attempt to commit the offences listed in (1) and (2) above is punished with the same penalties.

10. Article 550**bis** of the Criminal Code punishes any (attempt) of external hacking, *i.e.* any attempt to gain access to a computer systems or to maintain such access, by someone who knows he/she is not authorized to gain such access.

The preparatory documents to the Act of 28 November 2000, introducing Article 550**bis** into the Criminal Code, as well as the other provisions on computer criminality, define "computer system" as: *"any system which allows the user to store, process or transmit data. This includes, in particular computers, chips, smart cards, networks and their components as well as telecommunications systems and their components which use information technology."* The 3DS is a "**computer system**" in the sense of Article 550**bis** of the Criminal Code.

Further, as explained above, it follows from the notifications made by Nintendo to the users, as well as from the 3DS's shell and protection measures, that users are **not authorized** to access the 3DS.

"Neimod"'s statements in the IRC conversations and in relation to the photographs posted on the Internet sufficiently evidence that the defendant has accessed (or at least, has been trying to access) the 3DS. The mere attempt to hack a computer system constitutes a criminal offence under Article 550**bis** of the Criminal Code.

As this acting involves breaking user licences, physical and technological protection measures, the defendant can only have acted knowingly. This is also confirmed by the vocabulary used by "Neimod", which includes clear references to "hacking", "haxx", etc.

Given the fulfilment of all the requirements set out in Article 550**bis** (1) and/or (4) of the Criminal Code, the offence of "hacking" or "attempt of hacking" must be upheld.

A. RE-USING OF DATA OR DAMAGE TO THE COMPUTER SYSTEM OR DATA (ARTICLE 550**BIS** (3) 1° CRIMINAL CODE)

Belgian Criminal Code, Article 550**bis** (3) 1° and 3°:

Anyone who falls into one of the situations listed in [Article 550**bis**] (1) [...] above [*i.e.*

external hacking], and who:

1° either re-uses in any way the data stored, processed or transmitted by the computer system;

2° [...]

3° or causes any sort of damage, whether intentionally or unintentionally, to the computer system or to the data stored, processed or transmitted by the computer system; will be punished by between 1 and 3 years' imprisonment and/or a fine of between 26 and 50,000 euros."

11. In the present matter, the defendant has been re-using the data stored and processed by the 3DS. Indeed, it is shown in the IRC conversation and follows from the process of hacking itself that he has gained access to the 3DS to obtain data that he uses to further hack the system, with the ultimate objective of being able to run unauthorized software on the 3DS (see, for example, the modified screen on the picture "WE HACKED IT!" above).

Similarly, the IRC conversations and photographs sufficiently show that the 3DS has been damaged.

Given that the conditions of Article 550*bis* (3) 1° and 3° are fulfilled, the aggravating circumstances referred to in these provisions must be upheld.

B. OWNING AND PRODUCTION OF 'HACKERTOOLS' (ARTICLE 550*BIS* (5) CRIMINAL CODE)

Belgian Criminal Code, Article 550*bis* (5):

(5) Anyone who illegally owns, produces, sells, obtains with the intention of using, imports or makes available in another form any device, including computer data, which was principally designed or adapted to commit the offences mentioned in (1) to (4) above, will be punished by between 6 months' and 3 years' imprisonment and/or a fine of between 26 and 100,000 euros.

12. The defendant's IRC conversations and photographs suggest that he has developed and/or owns tools designed or adapted to access the 3DS, in breach of Article 550*bis* (5) of the Criminal Code..

Accordingly, this offence should be further investigated.

C. CONCEALMENT OF DATA OBTAINED THROUGH HACKING (ARTICLE 550*BIS* (7) CRIMINAL CODE)

Belgian Criminal Code, Article 550*bis* (7):

(7) Anyone who, knowing that data was obtained by the commission of one of the offences mentioned in (1) to (3) above, holds them, reveals or divulges them to a third party, or uses them in any way, will be punished by between 6 months' and 3 years' imprisonment and/or a fine of between 26 and 100,000 euros.

13. It follows from the IRC conversations that the defendant has obtained data by accessing the 3DS. He is *holding* those data (knowing they were obtained by getting unauthorized access to the 3DS), which already fulfils the requirement set out in Article 550*bis* (7) of the Criminal Code. Besides, the reference to a “secret circle” in the IRC conversations gives indication of the fact that such data have been *revealed* and/or *divulged*. More broadly, the hacking advice “Neimod” is spreading in the IRC must also be interpreted as a divulcation of such data. Finally, as has already been established above, the defendant is *using* the data obtained by accessing the 3DS (to pursue further hacking activities).

There is accordingly no doubt that the offence laid down in Article 550*bis* (7) of the Criminal Code should be upheld.

D. (ATTEMPT OF) DATA OR SYSTEM SABOTAGE (ARTICLE 550TER (1) AND (6) CRIMINAL CODE)

Belgian Criminal Code, Article 550ter (1) and (6):

(1) Anyone who, knowing he is not authorized, directly or indirectly enters into a computer system, changes or deletes data, or changes their normal use in the computer system by any technological means, will be punished by between 6 months’ and 3 years’ imprisonment and/or a fine of between 26 and 25,000 euros.

If the offence mentioned in (1) above is committed with fraudulent intent [i.e., with a view to making profit] or with the intention of causing harm, the term of imprisonment will be between 6 months and 5 years. [...]

(6) Any attempt to commit the offence mentioned in (1) above will be punished by the same penalties.

14. It follows from the notifications made by Nintendo to the 3DS users, the 3DS’s shell and technological protection measures implemented into the 3DS, that the defendant was not authorized to “change or delete date” or to “change the normal use” of the 3DS. The defendant was clearly aware of the fact that, by breaking these barriers, he performed an activity which was not authorized. This is also confirmed by the vocabulary used in the IRC conversations, where references are made to terms such as “hacking or “haxx”. The IRC conversations and the photographs posted by the defendant on the Internet also show that “Neimod” modified the normal use of the 3DS. As a subsidiary argument, it must in any event be upheld that he *attempted* to do so.

Consequently, the offence laid down in Article 550ter (1) and/or (6) of the Criminal Code should also be upheld.

E. OWNING AND PRODUCTION OF TOOLS FOR SYSTEM SABOTAGE (ARTICLE 550TER (4) CRIMINAL CODE)

Belgian Criminal Code, Article 550ter (4)

(4) Anyone who illegally owns, produces, sells, obtains with the intention of using, imports, distributes or makes available in another form, a device including computer data which was principally designed or adapted to permit the commission of offences mentioned in (1) to (3) above, while knowing that these data could be used to cause harm to, or prevent the complete or partial normal functioning of, a computer system, will be punished by between 6 months' and 3 years' imprisonment and/or a fine of between 26 and 100,000 euros.

15. The IRC conversations involving the defendant and the photographs posted by the latter on the Internet suggest that he has developed tools and owns tools designed to enter, change or delete data of, or to change the normal use of, the 3DS, which violates Article 550ter (4) of the Criminal Code.

Accordingly, the aggravating circumstance referred to in Article 550ter (4) of the Criminal Code should be further investigated.

F. CIRCUMVENTION OF TECHNOLOGICAL PROTECTION MEASURES (ARTICLE 79bis (1), FIRST INDENT, OF THE COPYRIGHT ACT)

Article 79bis (1) of the Belgian Act of 30 June 1994 on copyright and neighbouring rights (the "Copyright Act")

Anyone who circumvents any effective technological protection measure, knowing, or having reason to believe that this circumvention could facilitate the committing of offences outlawed by Article 80, is guilty of an offence which is punished by the sanctions outlined in Article 81 and Articles 83 to 86. The circumvention of technological measures described in this Article or in Article 87bis, (1), is deemed to facilitate the committing of offences listed in Article 80.

(...)

The expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorized by the right-holder of any copyright or any right neighbouring right.

Technological measures shall be deemed "effective" pursuant to indent 1 and 2 where the use of a protected work or other subject-matter is controlled by the right-holders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

16. As stated above, Nintendo has applied technological protection measures to the 3DS and authentic 3DS games. These correspond to the definition of "effective technological protection measures" in Article 79bis (1) of the Copyright Act as they prevent, among other, to play unauthorized pirated copies of games.

The IRC conversations and the photographs posted on the Internet by the defendant show that he has circumvented Nintendo's technological protection measures. This is clearly evidenced by the photograph showing "WE HACKED IT!" displayed on the 3DS's screen, Indeed, in order to be able to have such a text displayed on the screen, the user

needs to inject a code into the console, which can only be achieved by circumventing the technological protection measures implemented by Nintendo.

17. The defendant recognized in the IRC conversations that by hacking the 3DS and by circumventing the technological protection measures implemented in the console, he would never be able to completely exclude the risk that third parties could eventually use the 3DS to play pirated games:

*13[2012/05/15 14:43:25] <neimod> and 3. I will try **my best** to never allow homebrew to run commercial games*
*15[2012/05/15 14:44:22] * Zaxuhe (~Zaxuhe@201-130-240-43-cable.cybercable.net.mx) Quit (Ping timeout: 504 seconds)*
[2012/05/15 14:44:58] <neimod> aka [read "also known as"] piracy

Thus, the defendant is well-aware that his action could facilitate offences of copyright infringement.

Accordingly, the offence laid down in Article 79 *bis* (1), first indent, of the Copyright Act should be upheld.

3. CIVIL CLAIM

18. Nintendo hereby files a complaint with registration of a civil claim in relation with the facts that have been outlined above.

Nintendo asks the Examining Judge to investigate further the above facts and to undertake all relevant investigation actions using all legally available powers, including but not limited to the seizure of all relevant evidence such as any computer material possessed by the defendant and any conversations available online involving "Neimod" and/or other Internet users.

The above mentioned offences are likely to cause significant harm to Nintendo on a commercial scale; the hacking of the 3DS would indeed enable third parties to play pirated games on the 3DS, which would cause a great loss of profit to Nintendo as a game developer and to third party publishers of 3DS games.

Moreover, Nintendo suffers harm as its reputation towards third party game developers, whose incentive to develop 3DS-compatible games would be seriously undermined if the console's security were attained, is tarnished by the defendant's activities.

19. Accordingly, Nintendo will claim compensation for all the damage resulting from the defendant's activities, based on Article 1382 of the Belgian Civil Code.

Nintendo will assess its damage further in the course of the criminal inquiry and subsequent proceedings.

Nintendo further respectfully requests that all materials used in relation with or for the commission of the above offences be seized, in order to prevent the occurrence of any further prejudice.

We thank you in advance for informing us of all further steps in this matter.

Sincerely yours,

For Nintendo,

Its counsel,

Olivier Vrins

EXHIBITS

- Statement of Nintendo electing domicile at its Counsel office for the proceedings;
- EFNET's #3dsdev IRC logs involving "Neimod"'s participation;
- Screenshots from "Neimod"'s Flickr® gallery.